Privacy Act

(Managerial Training)

United States Army

Overview

After completing this training managers should be familiar with the following:

- Managerial Responsibilities
- Breach Prevention and Mitigation
- Best Practices

Managerial Responsibilities

Privacy Officers:

- Are appointed at Headquarters Department of the Army (HQDA) and Command levels throughout the Army.
- Execute the privacy program in functional areas and activities under their responsibility.
- Ensure that Privacy Act records collected and maintained within the Command or activity are properly described in a Privacy Act system of records.
- Process reports of suspected Privacy Act Violations.
- Prepare a new, altered, amended, deleted or closed SORNs and submit them to the Army Privacy Office for review.

Managerial Responsibilities

Privacy Officers must ensure:

- No undeclared systems of records are being maintained.
- A Privacy Act Statement is provided to individuals when information is collected.
- Each Privacy Act system of records notice within their purview is reviewed biennially.

Managerial Responsibilities

A **System Manager** provides oversight and development of a system of records notice.

A System Manager must:

- Comply with AR 340-21, Army Privacy Program.
- Follow rules published in each system of records notice.
- Respond to First-Party Access and Amendment Requests.
- Determine if Third-Party Disclosures are authorized.
- Maintain an accounting of all Third-Party Disclosures.

Managerial Responsibilities

System Managers must ensure:

- Appropriate procedures and safeguards are developed, implemented, and maintained.
- All personnel with access to each system are aware of their responsibilities for protecting personal information being collected and maintained under the Privacy Act.
- Each Privacy Act system of records notice within their purview is reviewed biennially.
- Information systems managed by a government contractor must contain the Federal Acquisitions Regulation (FAR) clause in the contract.

Managerial Responsibilities

Contractor Managed Systems:

- The Federal Acquisitions Regulation (FAR) sets forth guidance that must be inserted in contracts when PII is managed by a government contractor.
- Information regarding the FAR clauses can be found in the Acquisition Guide at http://www.archives.gov/records-mgmt/toolkit/pdf/ID189.pdf
.

Managerial Responsibilities

Information Assurance Official:

- Provides a unified approach to protect information stored, processed, accessed, or transmitted by information systems.
- Consolidates and focuses Army efforts in securing information.
- Risk management approach for implementing security safeguards.

Breach Prevention and Mitigation

The Army has a responsibility to safeguard PII in its possession and to prevent its theft, loss, or compromise.

It is essential that all Army personnel, to include contractors, ensure their actions do not contribute to a compromise occurring if the agency is to retain the trust of those individuals on whom information is maintained.

Breach Prevention and Mitigation

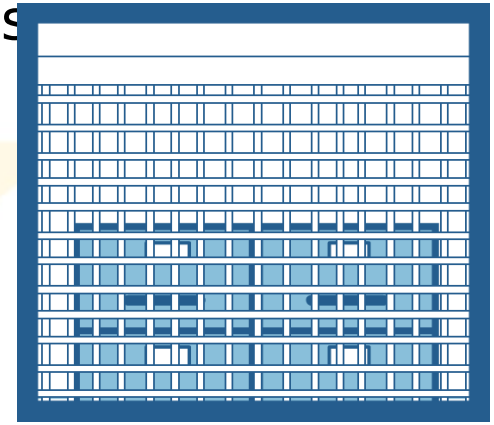
Managers should ensure their staff applies the appropriate breach prevention and mitigation safeguards.

Administrative Safeguards

- PII holdings inventory
- Policies and Procedures
- System of Records Notice
- Forms
- Privacy Act Statements
- Training
- Contract language
- Awareness campaigns

Breach Prevention and Mitigation

Managers should ensure their staff applies the appropriate breach prevention and mitigation safeguards.



Physical Safeguards

- Locked cabinets
- Door and building access control systems
- Installation physical access control systems
- User physical control of mobile devices
- Coversheets for documents containing PII
- Laptop locks

Breach Prevention and Mitigation

Managers should ensure their staff applies the appropriate breach prevention and mitigation safeguards.

Technical Safeguards

- Inventory of equipment
- CAC enabled laptops
- Email encryption
- Permission and access settings
- Automatic timeout screens
- System lockout

Breach Prevention and Mitigation

Managers will ensure the appropriate remedial action(s) are taken when PII is lost or compromised.

At a minimum, if PII is lost as a result of negligence or failure to follow established procedures, the individual(s) responsible will receive counseling and additional training reminding them of the importance of safeguarding PII.

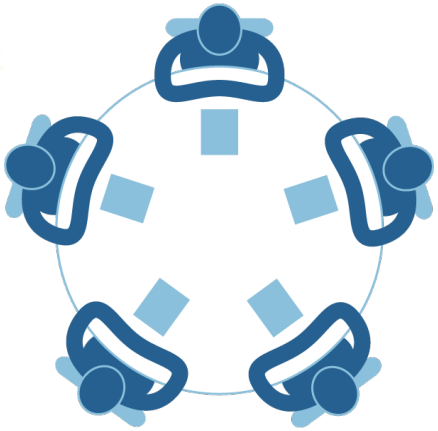
Breach Prevention and Mitigation

Additional remedial actions may include prompt removal of authority to access information or systems from individuals who demonstrate a pattern for error in safeguarding PII as well as other administrative or disciplinary actions.

Best Practices

Use Staff Meetings to stress good privacy practices:

- Voice your commitment to protecting individual privacy.
- Applaud workers who practice good privacy principles!
- Remind staff to use caution when posting data to shared drives and or multi-access calendars.
- Periodically review shared devices for compliance.



Best Practices

When discussing a person’s health, financial affairs, personnel actions,

criminal history, family affairs, or other personal aspects of his or her life, it

is important to remember that details should not be brought up in staff meetings or discussed in common areas.

Personal matters should never be discussed with anyone without a strict need to know.

References

Defense Privacy and Civil Liberties Office – http://dpclo.defense.gov

Army Regulation 340-21, “The Army Privacy Program”

DoD Directive 5400.11, “DoD Privacy Program”

DoD Regulation 5400.11-R, “Department of Defense Privacy Program”

DA&M Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”